Writing proofs for MATH 51H
Section 1: Universal statements, proof by contradiction, proof by induction

September 28, 2018

1 Introduction

A proof is a mathematical argument for why a statement is true. In contrast to more subjective disciplines, concepts in math have rigorous descriptions and deductions must be 100% logically sound. The purpose of writing a proof is to communicate your argument to others. Therefore, it is important for you to learn how to write clear proofs that other people can understand. Math involves a lot of writing, and the standards for grammar and clarity are the same as in any other field. In particular, always write in complete sentences.

Writing proofs is a separate skill from problem solving. When you do not have much experience writing proofs, many homework-type problems can appear to be much harder than they actually are. In these proof writing sections, we’ll cover the proof strategies you will need to know for this class so that this artificial difficulty disappears.

Today we will cover how to write proofs of universal statements and two general proof techniques: proof by contradiction and proof by induction. For each topic we’ll present a proof of a simple result and break down the purpose of each line, except in the section on induction, for which instead there is an extended explanation and proof template. There will also be a second proof example without the breakdown, and a collection of optional exercises.

2 Proving universal statements

Most mathematical statements that you’ll encounter in your life are universal statements. These statements say that for all elements in a particular set, some result holds. For example:

- The cube of an odd integer is odd.
- If \( n, m \in \mathbb{Z} \) and \( m \) is even, then \( nm \) is even.
- For \( n \in \mathbb{N} \), \( \sum_{j=1}^{n} j^3 = \frac{n^2(n+1)^2}{4} \) (HW 1)
- For any vectors \( x, y \in \mathbb{R}^n \), \( \|x - y\|^2 + \|x + y\|^2 = 2(\|x\|^2 + \|y\|^2) \) (HW 1)
are all examples of universal statements. If the set in question is finite, you can prove the statement by checking each individual element. However, if the set in question is infinite, then you cannot prove the statement by checking any number of individual elements. To prove the statement in this case, we need to argue using a general element of the set.

2.1 Examples

Proposition. The square of an even integer is a multiple of 4.

Proof. Let $a$ be an even integer. Then $a = 2 \cdot b$ for some integer $b$. We have $a^2 = (2 \cdot b) \cdot (2 \cdot b) = 4 \cdot b^2$. Because the product of two integers is an integer and $b$ is an integer, $b^2$ is an integer. This means that $a^2$ is the product of 4 and an integer, i.e. $a^2$ is a multiple of 4. Since $a$ was an arbitrary even integer, we conclude that the square of every even integer is a multiple of four.

We will now break down the proof.

<table>
<thead>
<tr>
<th>Let $a$ be an even integer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computing $2^2$, $4^2$, $6^2$, and $8^2$ and seeing that they are all multiples of 4 is not a proof, even though by computing these examples you may see why the proposition should be true. Our goal is to show that the square of every even integer is a multiple of four, and to do this we need a “general” even number. Any specific even number will not suffice, even if we check a million of them. We give our “general” even number the name “$a$” so that we can refer to it in our argument.</td>
</tr>
<tr>
<td>Then $a = 2 \cdot b$ for some integer $b$.</td>
</tr>
<tr>
<td>This is just a statement of the definition of an even number. Since $a$ is a “general” even number, the above is really the only information available for us to use. Because $a$ is a “general” even number, it is the product of 2 and a “general” integer, which we name “$b$” so that we can refer to it later.</td>
</tr>
<tr>
<td>We have $a^2 = (2 \cdot b) \cdot (2 \cdot b) = 4 \cdot b^2$.</td>
</tr>
<tr>
<td>We are interested in what the square of a “general” even number is, so we square our “general” even number $a$. The square turns out to be a nice expression, $4 \cdot b^2$.</td>
</tr>
<tr>
<td>Because the product of two integers is an integer and $b$ is an integer, $b^2$ is an integer.</td>
</tr>
</tbody>
</table>
Recall that our goal is to show that \( a^2 \) is a multiple of 4, since \( a \) is our “general” even integer. We have shown that \( a^2 = 4 \cdot b^2 \), so we’re done if \( b^2 \) is an integer, because then \( a^2 \) has the form of a “general” multiple of 4. You are free to use the fact that the product of two integers is again an integer without explanation. Because \( b^2 = b \cdot b \), \( b^2 \) is thus an integer.

This means that \( a^2 \) is the product of 4 and an integer, i.e. \( a^2 \) is a multiple of 4.

Putting together the two previous sentences, we see that \( a^2 \) has the form of a “general” multiple of 4. Compare and contrast this sentence with the second sentence of the proof. There we unravel the definition of an even number, and here we “reravel” the definition of being a multiple of 4.

Since \( a \) was an arbitrary even integer, we conclude that the square of every even integer is a multiple of four.

This line explains and justifies the inclusion of the first sentence of the proof, for we really have proved that the result holds for any even number. It is also good practice in to finish a proof by stating the result that you have just proved.

Here is a second example of a universal statement and its proof:

**Proposition.** The product of two rational numbers is rational.

*Proof.* Let \( \frac{a}{b}, \frac{c}{d} \in \mathbb{Q} \). We have

\[
\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.
\]

By definition, \( a, b, c, d \in \mathbb{Z} \) and \( b, d \neq 0 \). Since the product of two integers is an integer, \( ac, bd \in \mathbb{Z} \). Since neither \( b \) nor \( d \) is zero, \( bd \neq 0 \) as well. This implies that \( \frac{a}{b} \cdot \frac{c}{d} = \frac{p}{q} \), where \( p = ac \) and \( q = bd \) are integers and \( q \neq 0 \). That is, \( \frac{a}{b} \cdot \frac{c}{d} \) is a rational number. Thus, since \( \frac{a}{b}, \frac{c}{d} \in \mathbb{Q} \) were arbitrary rational numbers, we conclude that the product of two rational numbers is rational.

\[\square\]

### 2.2 Exercises

*Exercise* 1. Prove that the sum of two odd integers is even.

*Exercise* 2. Prove that the product of two integers which are perfect squares is a perfect square.

*Exercise* 3. Prove that the sum of two rational numbers is a rational number.

*Exercise* 4. If \( a, b \in \mathbb{Z} \), we say that \( a \) *divides* \( b \) if there exists a \( c \in \mathbb{Z} \) such that \( b = ac \). We use the notation \( a \mid b \) to mean that \( b \) divides \( a \). For example, \( 2 \mid 4, 3 \mid -6 \), and \( 13 \mid 143 \).
• Show that 1 divides any integer.
• Show that any integer divides 0.
• Show that if \( n \) is an odd integer, then \( 4 \mid n^2 - 1 \).
• Show that if \( a \mid b \) and \( a \mid c \), then \( a \mid (b + c) \).
• Show that if \( a \mid b \) and \( b \mid c \), then \( a \mid c \). That is, the divisibility relation is transitive.

3 Proof by contradiction

Suppose we want to prove some mathematical statement. One strategy is to show that if the statement weren’t true, then we’d be led to a conclusion that we know to be false. Thus, statement must be true, for assuming that it is false leads to a contradiction.

3.1 Examples

Proposition. If \( z \in \mathbb{R} \) is irrational, then so is \( -z \).

Proof. Let \( z \in \mathbb{R} \) be irrational. Suppose by way of contradiction that \( -z \) were rational. Then there exist \( p, q \in \mathbb{Z} \) with \( q \neq 0 \) such that \( -z = \frac{p}{q} \). But then \( z = -\frac{p}{q} = \frac{-p}{q} \). This implies that \( z \) is rational, which gives a contradiction since we assumed that \( z \) was irrational. \( \Box \)

We will now break down the proof.

Let \( z \in \mathbb{R} \) be irrational.

As in any proof of a universal statement, we take \( z \) to be an arbitrary irrational number.

Suppose by way of contradiction that \( -z \) were rational.

You should signal some way at the beginning of a proof by contradiction that this is the technique that you are planning to use. After we inform the reader of our strategy, we state the negation of the result that we are trying to prove. If \( z \) were not irrational, then it would be rational by definition.

Then there exist \( p, q \in \mathbb{Z} \) with \( q \neq 0 \) such that \( -z = \frac{p}{q} \).

This is the definition of what it means for \( z \) to be rational. Since we’re trying to derive a contradiction from \( z \) being rational, we should have to invoke the definition at some point.
But then \( z = \frac{-p}{q} = \frac{-p}{q} \).

There is nothing stopping \(-z\) from being rational when \( z \in \mathbb{R} \) is arbitrary, but the proposition we’re trying to prove has us assume that \( z \) is irrational. In fact, this is the only thing we’re assuming, so we must use it some time in the proof. We want to connect what we know about \(-z\) to what we know about \( z \) somehow. Since \( z \) is just \(-z\) times \((-1)\), \( z \) must be equal to \( -\frac{p}{q} = \frac{-p}{q} \).

This implies that \( z \) is rational, which gives a contradiction since we assumed that \( z \) was irrational.

The previous line told us that \( z \) can be written as the quotient of two integers \(-p\) and \( q, q \neq 0. \) So by definition, \( z \) is rational. But by hypothesis \( z \) is irrational. Since a number cannot be both rational and irrational, this is a contradiction.

**Proposition.** If \( 0 < x < 1 \), then \( \sqrt{x} > x \).

*Proof.* Let \( 0 < x < 1. \) Suppose by way of contradiction that \( \sqrt{x} \leq x \). Since \( x > 0, \sqrt{x} \neq 0, \) and hence dividing the inequality \( \sqrt{x} \leq x \) on both sides by \( \sqrt{x} \) shows that \( 1 \leq \sqrt{x} \). Squaring both sides, since both \( 1 \) and \( \sqrt{x} \) (being greater than or equal to \( 1 \)) are positive, we get that \( 1 \leq x \). This is a contradiction, for we assumed that \( x < 1 \). 

3.2 Exercises

*Exercise 5.* Let \( n \in \mathbb{Z}. \) Prove that if \( n^2 \) is even, then \( n \) is even.

*Exercise 6.* Prove that \( \sqrt{5} \) is irrational.

*Exercise 7.* Let \( z > 0 \) be irrational.

- Show that \( \sqrt{z} \) is irrational.
- Show that \( \sqrt{n} \) is irrational for all integers \( n \geq 3 \) as well.

4 Proof by induction

The second strategy that we’ll cover today is that of proof by induction. If you are interested in computer science, then this proof strategy will be very important to you in the future.

It is easiest to explain the method by presenting an example first. Let’s prove the equality

\[
1 + 2 + \cdots + 2^n = 2^{n+1} - 1.
\]

Checking it for the case \( n = 1 \) is easy: the left hand side is \( 1 + 2 = 3 \), and the right hand side is \( 2^{1+1} - 1 = 4 - 1 = 3 \) as well. Suppose that we have checked it by hand for \( n \) up to
10, and have gotten bored of all of the arithmetic. To prove it for the case $n = 11$, we just have to note that the left hand side is

$$(1 + 2 + \cdots + 2^{10}) + 2^{11},$$

and we have already computed $1 + 2 + \cdots + 2^{10}$: $2^{10+1} - 1 = 2^{11} - 1$. Hence,

$$1 + 2 + \cdots + 2^{11} = 2^{11} - 1 + 2^{11} = 2 \cdot 2^{11} - 1 = 2^{12} - 1,$$

and we have proved the result for $n = 11$. We can generalize this argument. Suppose that we have proved the claim for all integers $n \leq k$. That is, we have shown that

$$1 + 2 + \cdots + 2^n = 2^{n+1} - 1$$

for all integers $n \leq k$. Then we have all we need to prove the claim for $n = k + 1$, for

$$1 + 2 + \cdots + 2^{k+1} = (1 + 2 + \cdots + 2^k) + 2^{k+1},$$

and we know the result for $n = k$: $1 + 2 + \cdots + 2^k = 2^{k+1} - 1$. Thus, we can plug it in the equation above to get

$$1 + 2 + \cdots + 2^{k+1} = (1 + 2 + \cdots + 2^k) + 2^{k+1} = 2^{k+1} - 1 + 2^{k+1} = 2 \cdot 2^{k+1} - 1 = 2^{(k+1)+1} - 1,$$

which gives the claim when $n = k + 1$.

So we have shown that if the claim holds for $n = k$, then it also holds for $n = k + 1$. We have also shown that it holds for $n = 1$. Combining these together, we see that it holds for $n = 2$. Since it holds for $n = 2$, it must hold for $n = 3$. Similarly, since it holds for $n = 3$, it must hold for $n = 4$ as well, and so on. Thus, we have proved the claim for all $n \in \mathbb{N}$.

The general idea of a proof by induction is as follows. Suppose that we have some mathematical statement $P(n)$ for each integer $n = 1, 2, \ldots$. For example, $P(n)$ could be one of the following:

- $1 + 2 + \cdots + 2^n = 2^{n+1} - 1$
- $n$ can be written as a product of prime numbers
- An under-determined system of $n$ linear equations always has a nontrivial solution.

If we can show that

1. $P(1)$ is true
2. if $P(n)$ is true, then $P(n + 1)$ is true

then we can conclude that $P(k)$ is true for all $k \in \mathbb{N}$. Corresponding to this, a proof by induction consists of two parts: the base case and the induction step. In the base case, we prove that $P(1)$ (or $P(0)$, or $P(k)$ for whatever $k$ you want to start the induction at) is true. Usually this is very easy to verify. In the induction step, we prove that if $P(n)$ is true, then $P(n + 1)$ is true. Usually it is in this step that you have to do the work.

To help you stay organized, here is a template for writing a proof by induction:
Proof. We proceed by induction on $n$.

*Base case:* First we check that $P(1)$ is true.

proof of $P(1)$

Thus, $P(1)$ is true.

*Induction step:* Suppose that $P(n)$ is true for a general $n \geq 1$. We will show that $P(n+1)$ is true as well.

proof of $P(n+1)$

Thus, $P(n+1)$ is true. This completes the induction.

As a final remark, the assumption in the induction step (“$P(n)$ is true”) is called the *induction hypothesis* or the *inductive hypothesis*. See the textbook’s proof of the “Underdetermined system lemma” for an example of someone besides me using this terminology. During the “proof of $P(n+1)$” section of your induction proof, when you inevitably need to use the fact that $P(n)$ is true, you can just say “by the induction hypothesis...”.

### 4.1 Examples

**Proposition.** For all $n \in \mathbb{N}$, $4 \mid (5^n - 1)$.

*Proof.* We proceed by induction on $n$.

*Base case:* First we check the claim when $n = 1$. We have $5^1 - 1 = 4$, and certainly $4 \mid 4$, so the claim holds.

*Induction step:* Suppose that the claim holds for a general $n \geq 1$. We will prove that the claim holds for $n + 1$. We have

$$5^{n+1} - 1 = 5 \cdot 5^n - 1 = (4 + 1)5^n - 1 = 4 \cdot 5^n + (5^n - 1).$$

By the induction hypothesis, $4 \mid 5^n - 1$, and certainly $4 \mid 4 \cdot 5^n$. Thus, $4$ divides their sum. That is, $4 \mid [4 \cdot 5^n + (5^n - 1)] = 5^{n+1} - 1$. Thus, the claim holds for $n + 1$. This completes the induction.

Note that in the next example, the base case is $n = 0$, instead of $n = 1$ as above.

**Proposition.** Let $r \in \mathbb{R}$ with $r \neq 1$ and $n \in \mathbb{Z}$, $n \geq 0$. Then

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}.$$

*Proof.* We proceed by induction on $n$.

*Base case:* First we check the claim when $n = 0$. We have $\sum_{i=0}^{0} r^i = 1$ and $\frac{r^{0+1} - 1}{r - 1} = \frac{r^1 - 1}{r - 1} = 1$. So indeed

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}.$$

7
holds when \( n = 0 \).

**Induction step:** Suppose that the result holds for a general \( n \geq 0 \). We will now prove that the result holds for \( n + 1 \). We have

\[
\sum_{i=0}^{n+1} r^i = \left( \sum_{i=0}^{n} r^i \right) + r^{n+1}.
\]

By the induction hypothesis, \( \sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1} \), so

\[
\sum_{i=0}^{n+1} r^i = \left( \sum_{i=0}^{n} r^i \right) + r^{n+1} = \frac{r^{n+1} - 1}{r - 1} + r^{n+1} = \frac{r^{n+1} - 1 + (r - 1)r^{n+1}}{r - 1} = \frac{r^{n+1} - 1 + r^{n+2} - r^{n+1}}{r - 1} = \frac{r^{n+2} - 1}{r - 1}.
\]

Thus, the result holds for \( n + 1 \). This completes the induction.

4.2 Exercises

**Exercise 8.** Prove by induction that

\[
\sum_{i=1}^{n} (2i - 1) = 1 + 3 + \cdots + (2n - 1) = n^2.
\]

That is, the sum of the first \( n \) odd numbers equals \( n^2 \).

**Exercise 9.** Prove by induction that for all \( n \in \mathbb{N} \), \( 6 \mid (n^3 - n) \).

**Exercise 10.** Recall that the Fibonacci sequence is defined by \( f_0 = 1, f_1 = 1, \) and \( f_n = f_{n-1} + f_{n-2} \) for all \( n \geq 2 \). So, \( f_2 = 2, f_3 = 3, f_4 = 5, f_5 = 8 \), and so on. Prove the following facts about the Fibonacci sequence using induction:

- \( \sum_{i=0}^{n} f_i = f_{n+2} - 1 \) for all \( n \in \mathbb{Z}, n \geq 0 \).
- \( \sum_{i=0}^{n} f_i^2 = f_n f_{n+1} \) for all \( n \in \mathbb{Z}, n \geq 0 \).
- \( f_n^2 - f_{n+1} f_{n-1} = (-1)^{n-1} \) for all \( n \in \mathbb{Z}, n \geq 0 \).